(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 January 2003 (16.01.2003)

PCT

(10) International Publication Number
WO 03/005357 A1

(51) International Patent Classification[7]: G11B 20/00, G06T 1/00, H04N 1/32

(21) International Application Number: PCT/IB02/02741

(22) International Filing Date: 4 July 2002 (04.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0116496.1 6 July 2001 (06.07.2001) GB
02075291.1 24 January 2002 (24.01.2002) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BRONDIJK, Robert, A.** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **MAES, Maurice, J., J., J-B.** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: **DEGUELLE, Wilhelmus, H., G.**; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

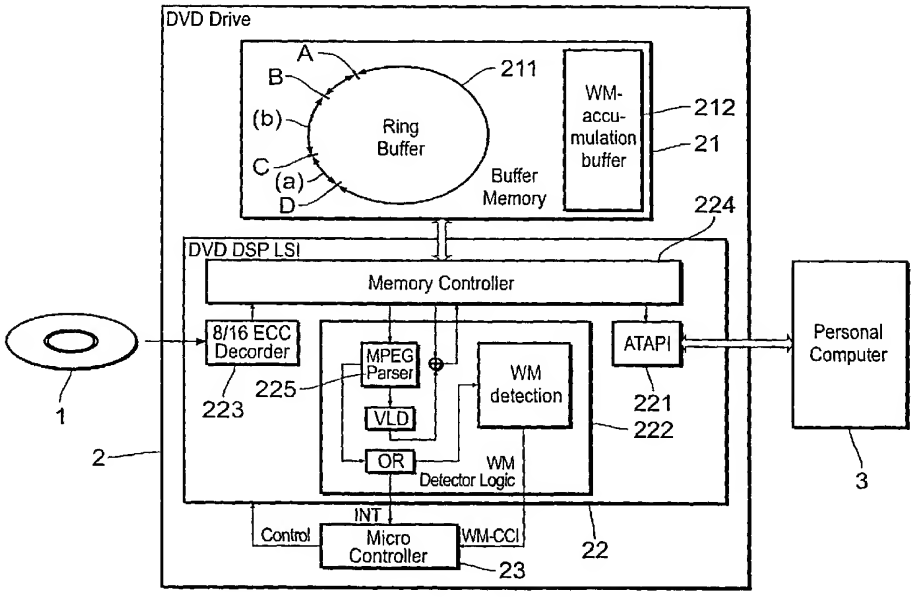
(81) Designated States *(national)*: CN, IN, JP, KR, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

**Published:**
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: METHOD FOR PROTECTING CONTENT STORED ON AN INFORMATION CARRIER




(57) Abstract: The invention relates to a method for protecting content comprising embedded copy protection data stored on an information carrier (1). In order to avoid that a user illegally circumvents a copy protection mechanism such as a watermark protecting said content to get an illegal access to said content, a method comprising the following steps is proposed: - reading content from or writing content to the information carrier in response to an access command, - storing said content in a memory, - continuing to read content from or to write content to the information carrier and accumulating (211, 212) said content in said memory until enough content is stored therein to extract and evaluate said copy protection data.

WO 03/005357 A1

# Method for protecting content stored on an information carrier

The invention relates to a method and a corresponding apparatuses for protecting content stored on an information carrier, to a computer program for performing the method and to an information carrier storing the computer program.

Nowadays, "embedded data" (also called "digital watermarking") is a technique used to embed copy control information in copyrighted material, such as music, movies and all kinds of audiovisual works. Watermarks may, for instance, be embedded in an audio or a video stream.

These watermarks may represent information indicating that the content, in which it is embedded, is e.g. never to be copied onto removable, optical media, or, indicating that the content should not be present on removable, optical media in unencrypted form. By way of example, a "Never Copy" video watermark, in unencrypted content on a recordable DVD disc, might be illegal, and might trigger a refusal to play back such content by compliant players. Another example is an audio watermark, indicating that content should only be recorded in encrypted form, which can be used to prevent the recording of audio content on a CD-RW, rewritable DVD or any other kind of optical disc.

Digital watermarking techniques typically require a significant amount of data to be examined before a reliable detection is possible. It may happen that several seconds of audio or video material, or derived data thereof, are being "accumulated", and that the detection is then performed on the accumulated data.

One way of embedding data in a copyrighted material is disclosed in International Application WO 99/45705, which document is hereby enclosed by reference. As the person skilled in the art is familiar with existing techniques for embedding data (or watermarking) and as the invention is not related to techniques for embedding data, no further information is given.

In the practical implementation of play control and record control rules in a PC environment, the inventors have identified several problems related to the specific operations of a PC drive, and to the fact that the user can control the operations of the drive.

A first problem identified by the inventors is that a user can try to circumvent play control, by sending multiple "read" commands to a drive, until the watermark (WM) is found. When the watermark is found and the "reading" is interrupted, the user can simply initiate new "read" commands from the same disc. Since watermark detection often requires a significant amount (seconds) of data to be read, such an attack may be feasible. Similarly, for record control, "write" commands can be sent until the watermark is detected, but after the interruption, the process is simply continued.

A second problem identified by the inventors is that drives need not "read" or "write" audiovisual information sequentially, but the drive can process random portions from an audiovisual work in random order. A hacker may write data to the drive while at the same time reading data from it. The purpose of this hack is to confuse the watermark detector by subjecting it to 2 different streams. The watermark detector may malfunction:

i. because of syntactic (MPEG) errors
ii. because of incompatible payloads of blocks that are read and written
iii. because it declares a watermarked stream unwatermarked (the watermark in one stream is diluted by the other non-marked stream)
iv. because it declares an unwatermarked streams watermarked (the watermark of the other stream affects the non-marked stream).

A third problem identified by the inventors is that it is possible to read or write protected data, using alternation of "read" and "write" actions of short pieces of content which are too small to allow for watermarks to be detected. The idea behind this hack is to do a "*butterfly*"-read (also known as "small read"): the desired (watermarked) sectors of video are not read contiguously, but interspersed with other data which is not (yet) desired. The intent of the hack is that the watermark detector never collects enough watermark energy between the "jumps" to create a decision above threshold. A derived scheme is one whereby the host reads the sectors in random order and permutes them back to the original order in the main memory. The same idea may be applied for writing watermarked data (copy-never or copy-no more) to a disc. In a straightforward implementation, a drive would then need two watermark detectors, which is expensive, or it would reset after each read or write action, thus enabling the described hack.

The invention has for an object to overcome the problems identified by the inventors, particularly the second and third problem, so as to avoid that a user illegally

circumvents a copy protection mechanism such as a watermark protecting said content and gets an illegal access to said content.

This object is achieved according to the present invention by a method as claimed in claim 1, comprising the steps of:

- reading content from or writing content to the information carrier in response to an access command,
- storing said content in a memory,
- continuing to read content from or to write content to the information carrier and accumulating said content in said memory until enough content is stored therein to extract and evaluate said copy protection data.

The invention is based on the idea not reset the watermark detector when different "read" or "write" commands are initiated, but to continue the "accumulation" of the data needed for a detection, regardless of the order in which segments are being read or written, and regardless of interruptions between these read or write actions from the same information carrier. Thus also the "alternate read-write" attack can be prevented by "accumulating" the audio or video data, regardless of whether it is coming from a "read" or "write" action. Copy protection information is collected until it can be completely evaluated so as to detect if it is e.g. allowed to read data from or to write data to the information carrier.

Preferred embodiments of the invention are defined in the dependent claims.

According to a first preferred embodiment the access to the information carrier is controlled on the basis of the extracted and evaluated copy protection information which preferably comprises a watermark which may comprise the information if and how often data read from the information carrier are allowed to be copied, if data are allowed to be written to the information carrier or if data have to be encrypted before writing it.

According to another aspect of the invention any new access commands such as read, write or copy commands during reading or writing content are delayed until in response to the previous access command enough content is accumulated and stored in the memory to extract and evaluate said copy protection data. In this way the above described problems where a hacker tries to avoid the detection of a watermark by small read or write commands or by mixing read and write commands can be effectively avoided. Any new command will not be executed before in response to a previous command the copy protection data from the content handled by the previous command is completely evaluated. A new access command may even not be dealt with if the copy protection data will then lead to a refusal of the access at all.

According to still another aspect of the invention, in case of a new access command during execution of a previous access command, a reset of the extraction and evaluation of the copy protection data is prevented until said copy protection data are completely extracted and evaluated. Usually, a watermark detector operating on a discontinuous stream would be resetted. Such a reset is prevented according to the present invention; instead a resynchronization is performed and content is further accumulated, e.g. into a fold-buffer of a watermark detector such that a watermark detection can be triggered if enough data is accumulated.

The proposed solution can be used in, but is not limited to, all PC drives which can read data from or write data to information carriers, particularly recordable or rewritable optical record carriers, such as CD, DVD or DVR information carriers. Such optical record carriers usually carry a unique number which can easily be used as identifier in the above described sense.

The invention relates also to an apparatus for protecting content stored on an information carrier as claimed in claim 7 comprising a reading unit, a memory, a control unit and a copy protection evaluation unit. Further, the invention relates to a personal computer comprising a drive as claimed in claim 8, a computer program as claimed in claim 9 and an information carrier as claimed in claim 10 storing a computer program as claimed in claim 9.

The invention will now be explained in more detail with reference to the drawings, in which:

Fig. 1 illustrates the problem of butterfly-reading,

Fig. 2 shows a block diagram of an apparatus according to the invention and

Fig. 3 shows a block diagram of a watermark detector.

By way of an example, the following preferred embodiment of a video watermark in the DVD "Copy Never" context is described.

In general, a DVD PC drive only understands "read command + data" and "write command + data". The data is always transmitted in units of 2KB (this is called a sector), in a maximum burst of 32 sectors (under Windows and most other operating systems). This implies that a drive has no notion of large contiguous sequences like a video recorder. For this reason, the watermark guidelines have to be tailored to speak in terms of "sectors", "read" and "write".

Fig. 1 illustrates the problem to be solved by the present invention. Shown are a disc 1, a DVD drive 2 for accessing the disc 1 and a PC 3 for processing the data read from the disc 1 by the drive 2. It is assumed that the disc 1 comprises an illegal copy of a CSS (Content Scrambling System) DVD-Video. Shown are further a frame 11 of 10 ECC blocks containing one I-picture including a "copy never" watermark. Usually said 10 ECC blocks #N to #N+9 of said frame 11 are read subsequently and processed further. A watermark detector present within the drive 2 would then be able to extract the watermark embodied in said data 11 and to evaluate it. Since the watermark is "copy never" it would then be prevented that said data are further copied by the PC 3.

To avoid this the desired (watermark) sectors of video of the frame 11 are not read contiguously, but interspersed with other data which is not (yet) desired. As a particular example illustrated in Fig. 1, after every desired sector of the frame 11, the PC 3 always requests via the drive 2 a (fixed) dummy sector 12 having serial number #N+j including another video pack V_pck. Said alternate reading of single blocks of the frame 11 and the dummy block 12 leads to a data stream 13 stored in the buffer memory 21 of the drive 2. Since therein each second block contains data of a different data stream, i.e. from either an I-picture (I) or from another video pack (V_pck) a watermark detector (not shown) included in the drive never collects enough watermark energy between the "jumps" to create a decision above threshold, i.e. a watermark embodied in the data stream can not be extracted and evaluated.

Within the PC 3 the dummy block 12 is then removed from the datastream 13 in the PCs main memory so as to reconstruct the original data stream 11 which may then be stored in a hard disc drive (HDD) 31 from which a backup of the hacked data can be stored on another disc 4.

A derived scheme is one whereby the host reads the sectors in random order and permutates them back to the original order in the main memory of the host. The same hack can be applied for writing watermarked data (copy-never or copy-no more) to a disc. This would, however, only work well for rewritable media but not for a write once (recordable) media. For the latter media there is no possibility to overwrite. Moreover, there is a limitation to the number of jumps or seamless links that can be created on a disc during the writing process.

Another hack based on a similar idea mixes read and write commands when accessing a disc. Thus the watermark detector shall be confused by subjecting it to two

different data streams at the same time so that again a watermark can not be extracted and evaluated.

Fig. 2 shows an apparatus for protecting content stored on an information carrier according to the present invention. As in Fig. 1 a PC 3 is used to access an information carrier, in this case a disc 1, via a drive 2 including the apparatus for protecting the content stored on the disc 1. It should be noted that the drive 2 can be a separate device as shown in Fig. 2, but can also be integrated into the PC 3, such as a PC disc drive.

The drive 2 comprises a buffer memory 21 a signal processor 22 and a micro controller 23. The buffer memory 21 comprises a ring buffer 211 for storing the data read from the disc 1 or to be written to the disc 1 and a watermark accumulation buffer 212 for accumulating watermark data extracted from the data read from the disc 1 or to be written to the disc 1 and to be used for evaluation of the watermark. The signal processor 22 comprises an interface (ATAPI) 221 to the PC 3, a watermark detector logic 222 for detecting and evaluating a watermark, an ECC decoder 223 for reading data from the disc and decoding it and a memory controller 224 for controlling said elements of the signal processor 22 and the buffer memory 21. Further a microcontroller 23 is provided for control of the signal processor 22 based on a detected watermark.

According to the present invention the drive 2 reads the non-contiguous sectors from the disc 1 and transfers them to the host 3, like in drives without watermark detectors 222. This means that the watermark detector 222 operates on a discontinuous MPEG-stream. Usually this would reset the watermark detector. According to the present invention, however, the watermark detector 222 resynchronizes and keeps accumulating the data into the fold-buffer of the watermark-detector. When enough data is accumulated, a watermark detection (SPOMF etc.) is triggered, and only then the fold-buffer is flushed.

Requesting even a single sector in most drive-architectures leads to reading ahead much more data of the drive, at least 32k bytes (1 ECC block is the smallest access unit for the error-correction system), but generally much more because most likely the host will request the following sectors next. Therefore, the MPEG-stream supplied to the watermark detector 222 can have relatively long stretches without breakes. In the ring buffer 211(a) indicates a sector requested by the host 3 and (b) indicates the data which the detector 222 may continue to parse.

When the host 3 requests a new sector, at some point the data in the ring buffer 211 is overwritten before the watermark detector 222 can process is. According to the invention the detector 222 continues until the parser 225 which is part of the detector 222

resynchronizes and continues folding/accumulating until it has enough MPEG-data for a watermark detection. In view of the resynchronization, the amount of folded content should be increased to $T_c$ seconds, which is the amount of video to be folded in case of a non-contiguous MPEG-stream.

In the ring buffer 211 marker A indicates a raw write pointer from which data from the disc is written into the buffer memory. Data from a corrected write pointer B has been ECC corrected. Data up to ATAPI-read pointer C has been transferred to the host 3. The MPEG-parser 225 in the watermark detector 222 has finally reached the MPEG-parser pointer D.

According to an alternative embodiment the drive 2 performs a read ahead of X bites, X being the amount of data to be read, of the requested data sectors in case of suspect MPEG-video, when suspect MPEG sector-data is requested by the host, and ensures that the watermark detector 222 can process this content. Only then, the drive 2 executes the new request from the host 3. This has the advantage of improved drive performance, i.e. the host does not have to wait for one complete watermark detection, and improved watermark detection, i.e. the sections of continuous MPEG data will be longer. The consequence is that the fold-buffer of the watermark detector is deleted with possibly non-watermarked material, i.e. is deleted from e.g. dummy sectors #N+j shown in Fig. 1.

For write-once media the same method can be applied: the host 3 must write data to the disk 1 in a (more or less) continuous way so that the watermark detector 222 can operate on the drive buffer 21. In practice, these problems may not be too large as a rewritable disc in which almost every ECC block has been written in separate write actions is likely to not function due to the extra link errors.

The invention is also applied to overcome the above described third problem of using mixed read and write commands at the same time. The watermark detector 222 parses both the data in the read-buffer and write-buffer and accumulates/folds both into the same fold-buffer. This will delete the watermark if one stream is watermarked and the other is not. For this reason the amount of detected content has to be increased to X kbytes. Such processing of both streams at the same time with one watermark detector does not lead to false-positives for honest users. Regardless of whether the read-action or the write-action was illegal, content has been transferred to/from the disc in unapproved way, and the disc should therefore be ejected.

Fig. 3 shows the general layout of a watermark detector. In a fold buffer incoming data, e.g. video data, is folded or accumulated, the buffer being a 128 x 128 buffer.

After 1 second of video data, a 2D Fourier transformation is performed in a FFT unit 41. In a SPOMF unit 42 a watermark detection is applied by replacing buffer element $z_i$ by $z_i / |z_i|$. In a correlation unit 43 the result is correlated with the watermark pattern 44 by performing a dot-product. Thereafter a 2D IFFT is applied in a IFFT unit 45. In search units 46 and 47 the highest peak and the second highest peak (in the sense of their absolute value) are searched. Finally, in a combination unit 48 their relative position vector of these two peaks is combined into a payload. For the payload to be valid this relative vector must lie on a predetermined grid of 128 allowed positions. If so, one considers this a valid micro-decision. For a watermark to be detected a valid macro-decision is needed. Such a valid macro-decision occurs when a single micro-decision with valid payload and two high peaks exceeding threshold $T_1$ appear or two single micro-decisions with valid and equal payload of two medium-sized peaks exceeding threshold $T_2$ appear. These two positive micro-decisions have to occur within 60 seconds of each other.

According to this preferred embodiment, the following watermark detection strategy is used. The data drive is to "accumulate" all of the sectors containing DVD video it encounters, independent on whether the sector was transferred in a read or in a write action. The accumulation continues until there is sufficient material for a watermark detection to be performed. This accumulation phase is followed by an analysis phase. If the analysis results in a positive recognition of a watermark, then the drive must feedback this, in some manner, to the user. If the disc is a recordable disc, the drive will then remember its unique disc ID. The unique disc ID will be coupled, in the drives' flash memory, with a number "n", which is the number of times a watermark has been found on that disc. If that number exceeds a number "N", all read and write actions will be blocked of that disc for a period of time. What that period of time is, may be influenced by a number of factors: the number of discs a drive can remember or the last time the drive was completely flashed. In any case, the number "N" (a practical value may be 10) is too small for a user to clandestinely copy a movie of several minutes, yet it is large enough for the user to either delete all of his illegal material or copy his legal material from the disc. The only way a user can make a disc, for which n>=N, usable again is to let the drive successfully execute a "format unit" command. After reformatting the disc, the drive must then delete that disc ID from its list of illegal discs. In this way, a user is able to reinstate a previously illegal disc.

The way drives can feedback to the user that a WM has been found could be by the drive giving a "check condition" and placing a new sense code in the sense buffer which tells the user that a "WM Copy Never has been detected". There after, the drive may

choose to e.g. perform a "tray-out" or a pause so that the user clearly realizes that something is wrong and that his transfer action is clearly interrupted.

This preferred embodiment can be summarized as follows:

(accumulation phase:)

- the drive accumulates sectors of video information, regardless of the order in which they are read or write,
- the drive accumulates sectors of all transferred data, hence for both read as write,
- the drives accumulates until it has sufficient material for the analysis phase

(analysis phase:)

- if a "Never Copy" WM is detected, then the drive shall look if the disc ID is present in the memory, otherwise it will create an entry, in which case "n" = 0,
- the corresponding "n" will be incremented,
- the PC drive may choose to perform a "tray-out" (i.e. the removing of the disc from the drive) or a pause,
- if "n">="N", then no read or write actions will be allowed, only the SCSI command "FORMAT UNIT" and the drive will send a "check condition" to the host and place a "Never Copy WM" in the sense buffer (the "sense buffer" is the information which a drive will send to the host in response to the SCSI command "REQUEST SENSE").

After a disc has been inserted, the drive will look at its disc ID and check if it appears in its database present in the memory. If that disc is already in the database and "n">="N", the actions as above will be taken.

CLAIMS:

1. A method for protecting content comprising embedded copy protection data stored on an information carrier, comprising the steps of:
- reading content from or writing content to the information carrier in response to an access command,
- storing said content in a memory,
- continuing to read content from or to write content to the information carrier and accumulating said content in said memory until enough content is stored therein to extract and evaluate said copy protection data.

2. The method according to claim 1, wherein access to said information carrier is controlled on the basis of the extracted and evaluated copy protection information.

3. The method according to claim 1, wherein said copy protection data comprises a watermark.

4. The method according to claim 1, wherein any new access commands during reading or writing content are delayed until in response to the previous access command enough content is accumulated and stored in the memory to extract and evaluate said copy protection data.

5. The method according to claim 1, wherein, in case of a new access command during execution of a previous access command, a reset of the extraction and evaluation of said copy protection data is prevented until said copy protection data are completely extracted and evaluated.

6. The method according to claim 1, wherein said information carrier is an optical record carrier, in particular a recordable or rewritable optical record carrier.

7. An apparatus for protecting content comprising embedded copy protection data stored on an information carrier, comprising:
- a reading unit for reading content from or writing content to the information carrier in response to an access command,
- a memory for storing said content,
- control means for controlling access to the information carrier such that the reading unit continues to read content from or to write content to the information carrier and accumulates said content in said memory until enough content is stored therein to extract and evaluate said copy protection data, and
- a copy protection evaluation unit for extracting said copy protection data from the content stored in said memory and to evaluate said extracted copy protection data.

8. A personal computer comprising a drive for accessing an information carrier, said drive comprising an apparatus for protecting content stored on said information carrier according to claim 7.

9. Computer program comprising program code means for performing the steps of anyone of the methods as claimed in claims 1 to 6.

10. Information carrier storing a computer program as claimed in claim 9.

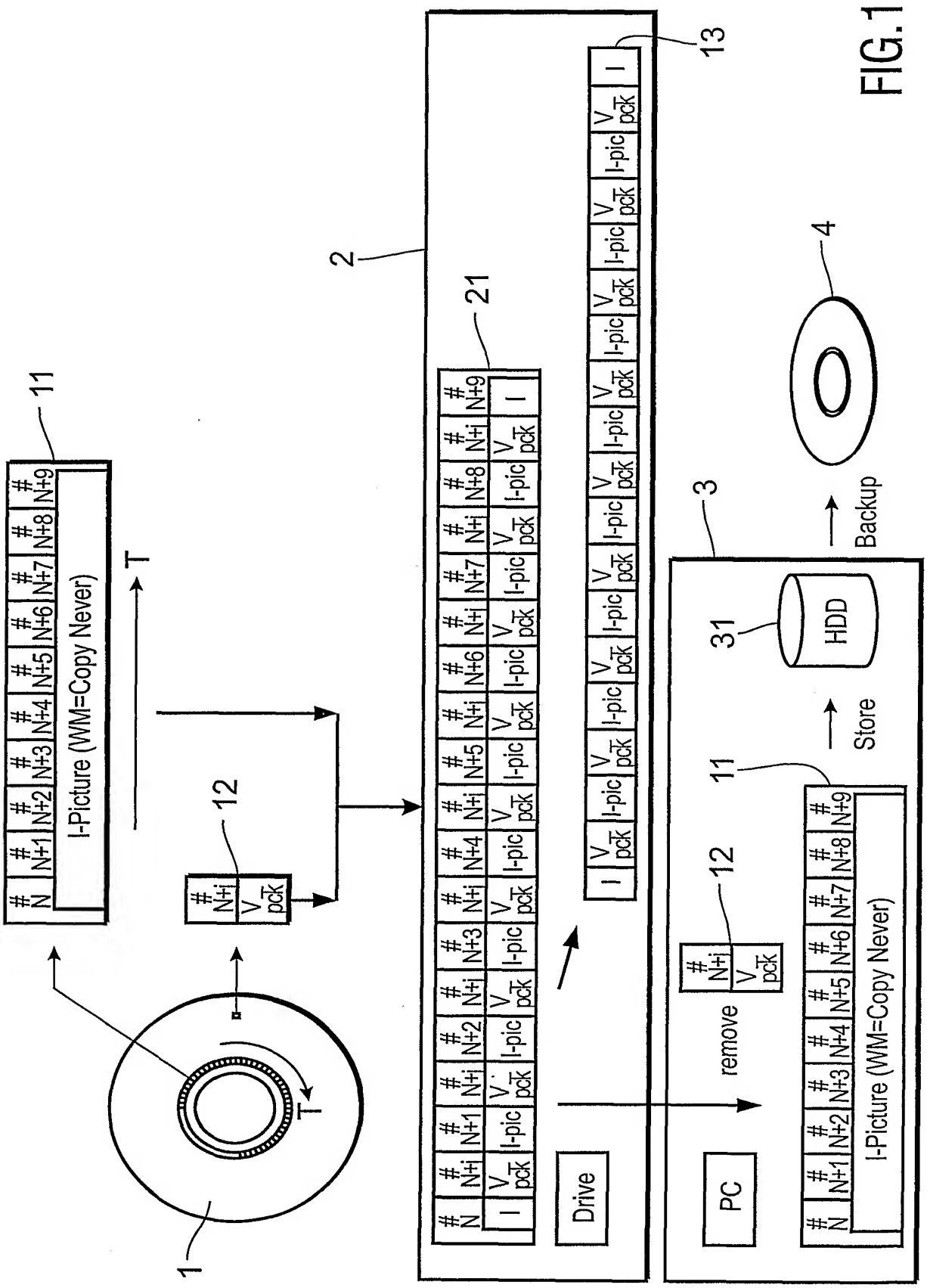

1
2
3
4
11
12
13
21
31
T
I-Picture (WM=Copy Never)
Drive
PC
remove
Store
HDD
Backup

FIG.1

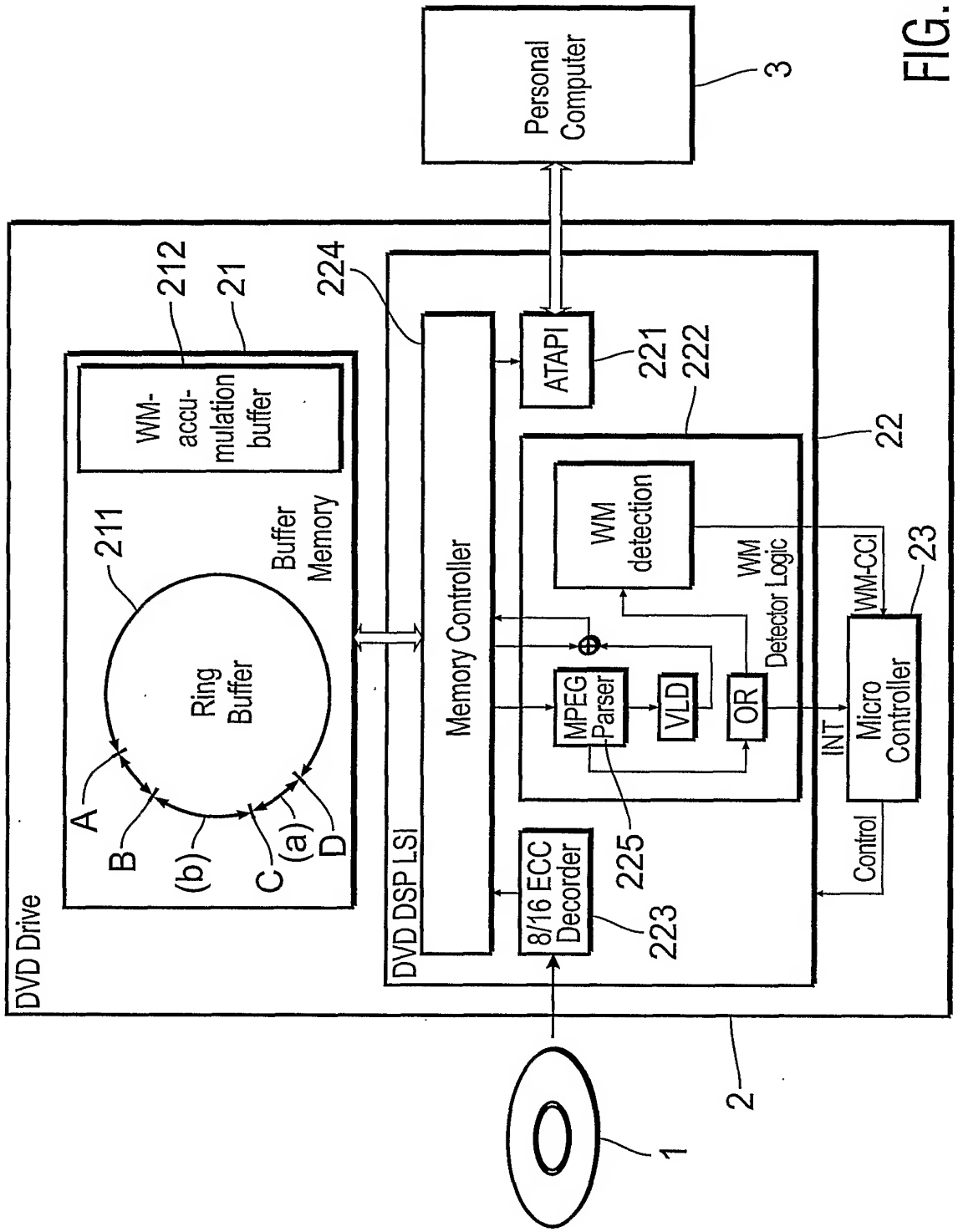

Personal Computer
3
DVD Drive
212
21
224
WM-accu-mulation buffer
Buffer Memory
211
Ring Buffer
A
B
(b)
C
(a)
D
DVD DSP LSI
Memory Controller
ATAPI
221
222
22
WM detection
WM Detector Logic
MPEG Parser
VLD
OR
INT
Micro Controller
WM-CCI
23
Control
8/16 ECC Decorder
225
223
2
1

FIG.2

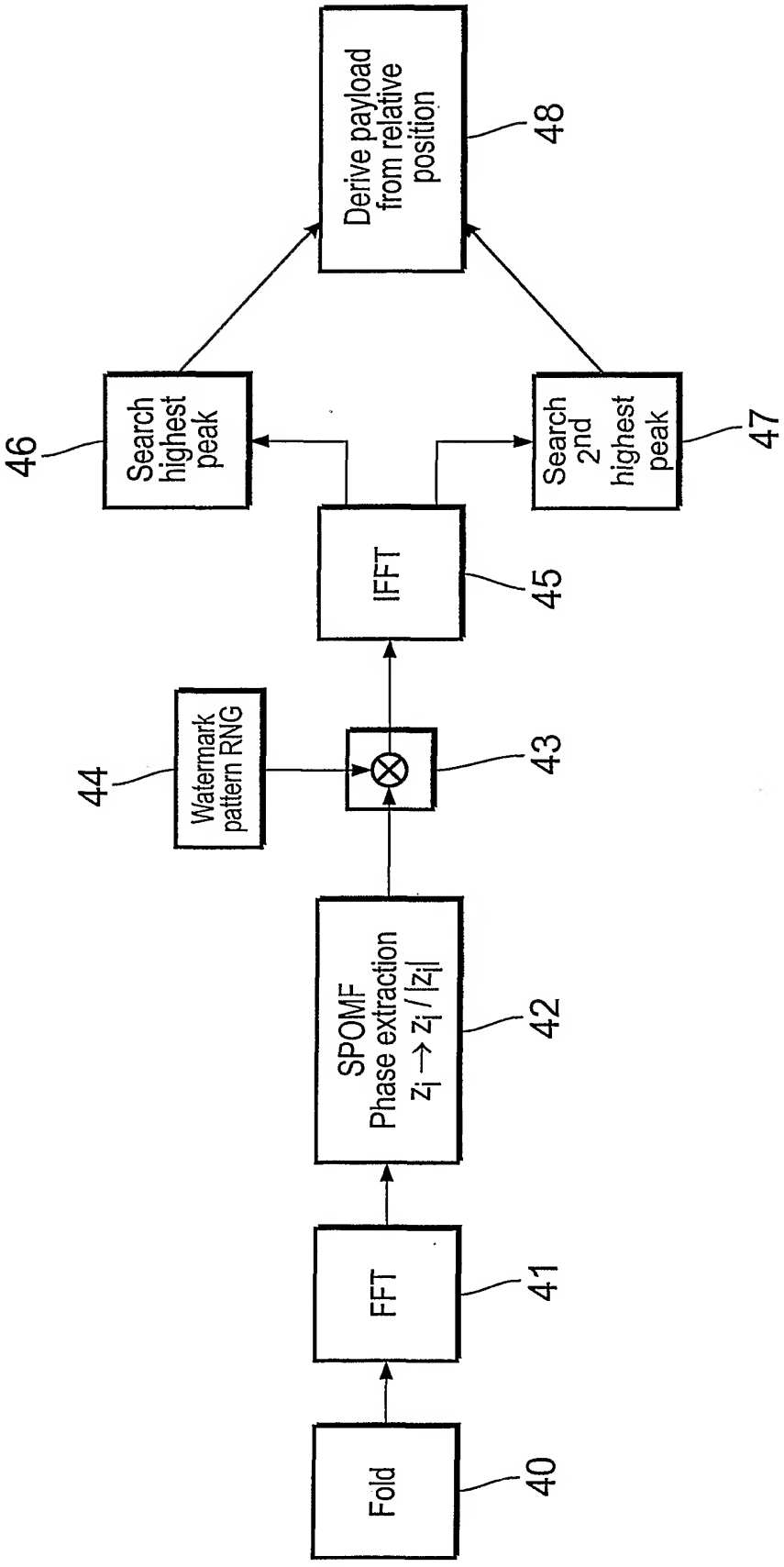

Fold
40
FFT
41
SPOMF
Phase extraction
$z_i \rightarrow z_i / |z_i|$
42
Watermark pattern RNG
44
43
IFFT
45
Search highest peak
46
Search 2nd highest peak
47
Derive payload from relative position
48

FIG.3

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 02/02741

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G06T1/00 H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B G06T H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | WO 00 04722 A (KONINKL PHILIPS ELECTRONICS NV) 27 January 2000 (2000-01-27)<br>page 2, line 18 - line 27<br>page 3, line 30 -page 5, line 7<br>figures 1,3 | 1-3,7-10 |
| X | EP 1 102 485 A (HITACHI LTD)<br>23 May 2001 (2001-05-23) | 1,3 |
| A | column 3, line 15 - line 25<br>column 4, line 45 -column 5, line 5<br>column 8, line 40 -column 10, line 5<br>figures 1-3 | 7-9 |

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 5 December 2002 | 23/12/2002 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | Schiwy-Rausch, G |

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X,P | EP 1 136 946 A (NIPPON ELECTRIC CO) 26 September 2001 (2001-09-26) abstract column 9, line 11 - line 22 column 11, line 26 - line 35 column 19, line 42 -column 22, line 30 figures 2-7 --- | 1-3,7-10 |
| X,P | US 2001/032313 A1 (HAITSMA JAAP ANDRE ET AL) 18 October 2001 (2001-10-18) page 5, line 13 -page 6, line 17 claim 7; figure 5 --- | 1-4,7-10 |
| Y | WO 99 45704 A (KONINKL PHILIPS ELECTRONICS NV ;MAES MAURICE J J J B (NL); PHILIPS) 10 September 1999 (1999-09-10) cited in the application page 1, line 13 - line 29 page 7, line 15 - line 20 --- | 1-3,6-10 |
| Y | VEEN VAN DER M ET AL: "ROBUST, MULTI-FUNCTIONAL AND HIGH-QUALITY AUDIO WATERMARKING TECHNOLGOY" PREPRINTS OF PAPERS PRESENTED AT THE AES CONVENTION, XX, XX, vol. 110, no. 5345, 12 May 2001 (2001-05-12), pages 1-9, XP001086463 Amsterdam, NL page 3, left-hand column, line 17 -page 4, left-hand column, line 25 --- | 1-3,6-10 |
| Y | KALKER T ET AL: "Analysis of watermark detection using SPOMF" IMAGE PROCESSING, 1999. ICIP 99. PROCEEDINGS. 1999 INTERNATIONAL CONFERENCE ON KOBE, JAPAN 24-28 OCT. 1999, PISCATAWAY, NJ, USA,IEEE, US, 24 October 1999 (1999-10-24), pages 316-319, XP010369137 ISBN: 0-7803-5467-2 page 1, right-hand column, line 15 - line 24 page 2, left-hand column, line 20 - line 37 --- -/-- | 1-3,6-10 |

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| P,A | ANONYMOUS: "Video Watermarking content protection technology" INTERNET ARTICLE, 'Online! December 2001 (2001-12), XP002223003 Retrieved from the Internet: <URL:http://www.studio-systems.com/broadfeatures/NovDec2001/VIDEO%20WATERMARKING%20CONTENT%20PROTECTION%20TECHNOLOGY/26.htm> 'retrieved on 2002-08-06! the whole document | 1 |
| A | M. FRIEDLINGER: "Automatisierte Segmentierung und Volumetrie bispektraler Magnetresonanz-Bilddaten des Gehirns" INTERNET ARTICLE, 'Online! September 1998 (1998-09), pages 157-164, XP002223004 Retrieved from the Internet: <URL:http://www.ubka.uni-karlsruhe.de/cgi-bin/psgunzip/1999/elektrotechnik/2/2.pdf> 'retrieved on 2002-08-06! page 161, paragraph B.2 -page 163, paragraph B.2.2 | |
| A | JONG WON SEOK ET AL: "Audio watermarking for copyright protection of digital audio data" ELECTRONICS LETTERS, 4 JAN. 2001, IEE, UK, vol. 37, no. 1, pages 60-61, XP002223005 ISSN: 0013-5194 | |
| A | IN-KWON YEO ET AL: "Modified Patchwork Algorithm: a novel audio watermarking scheme" PROCEEDINGS INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY: CODING AND COMPUTING, PROCEEDINGS INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY: CODING AND COMPUTING, LAS VEGAS, NV, USA, 2-4 APRIL 2001, pages 237-242, XP002223006 2001, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-7695-1062-0 | |
| T | ANONYMOUS: "Watermarking and Applications" INTERNET ARTICLE, 'Online! XP002223007 Retrieved from the Internet: <URL:http://contentprotection.broadcastengineering.com/watermarking_and_applications/> 'retrieved on 2002-08-06! figure 2 | |

-/--

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 02/02741

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| T | JONGWON SEOK ET AL: "A novel audio watermarking algorithm for copyright protection of digital audio" ETRI JOURNAL, JUNE 2002, ELECTRON. & TELECOMMUN. RES. INST., TAEJON, SOUTH KOREA, vol. 24, no. 3, pages 181-189, XP002223008 ISSN: 1225-6463 | |

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 02/02741

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 0004722 A | 27-01-2000 | CN 1273747 T | 15-11-2000 |
| | | WO 0004722 A1 | 27-01-2000 |
| | | EP 1038402 A1 | 27-09-2000 |
| | | JP 2002521881 T | 16-07-2002 |
| | | TW 395133 B | 21-06-2000 |
| EP 1102485 A | 23-05-2001 | JP 2001210013 A | 03-08-2001 |
| | | EP 1102485 A2 | 23-05-2001 |
| EP 1136946 A | 26-09-2001 | JP 2001275115 A | 05-10-2001 |
| | | EP 1136946 A2 | 26-09-2001 |
| | | US 2001026616 A1 | 04-10-2001 |
| US 2001032313 A1 | 18-10-2001 | WO 0157868 A1 | 09-08-2001 |
| WO 9945704 A | 10-09-1999 | AU 2437499 A | 20-09-1999 |
| | | CN 1266586 T | 13-09-2000 |
| | | CN 1266587 T | 13-09-2000 |
| | | CN 1269098 T | 04-10-2000 |
| | | CN 1269099 T | 04-10-2000 |
| | | EP 0981900 A2 | 01-03-2000 |
| | | EP 0981901 A2 | 01-03-2000 |
| | | EP 0981902 A2 | 01-03-2000 |
| | | EP 0981903 A2 | 01-03-2000 |
| | | WO 9945704 A2 | 10-09-1999 |
| | | WO 9945705 A2 | 10-09-1999 |
| | | WO 9945706 A2 | 10-09-1999 |
| | | WO 9945707 A2 | 10-09-1999 |
| | | JP 2001525151 T | 04-12-2001 |
| | | JP 2002503431 T | 29-01-2002 |
| | | JP 2001525152 T | 04-12-2001 |
| | | JP 2001525153 T | 04-12-2001 |
| | | PL 336841 A1 | 17-07-2000 |
| | | PL 336845 A1 | 17-07-2000 |
| | | US 6477431 B1 | 05-11-2002 |